Revised Claims

1. A decoder device (STB) having a control unit (RCU) for decrypting encrypted television programs, comprising
- an input (4) for feeding in an encrypted television program;
- a decryption device (DVB), which decrypts an encrypted television program into a format that can be reproduced by a television set (TV);
- an output (2), which can be connected to a television set (TV) in order to feed the decrypted television program into the television set (TV) for reproduction;
- an interface (IFD 3,6) for an identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB); and
- an interface (IR 3,6) for a control unit (RCU) of the decoder device (STB); and
- an interface (BC 5) to a telecommunications network (tel. network);
characterized in that
- the interface (IFD 3,6) for the identification and/or key carrier component (ICC DVB) is arranged in the control unit (RCU) of the decoder device (STB); and
- an interface (IFD 3,6) to an identification and/or key carrier component (ICC BC) is present, a connection being established via the telecommunications network (tel. network) to a specific subscriber as a function of an authorization by the identification and/or key carrier component (ICC BC).

2. The decoder device having a control unit (RCU) as recited in Claim 1, characterized in that
- the interface (IFD 3,6) to the identification and/or key carrier component (ICC BC) for authorizing the

connection via the telecommunications network (tel. network) is arranged in the control unit (RCU).

3. The decoder device (STB) having a control unit (RCU) as recited in Claim 1 or 2, characterized in that
- the control unit (RCU) is also set up for controlling the television receiver (TV set), which has an interface (IR 9) for receiving control commands.

4. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that
- the identification and/or key carrier component (ICC BC) for authorizing the connection via the telecommunications network (tel. network) and the identification and/or key carrier component (ICC BVB) for enabling the encryption device (DVB) are implemented either by two separate or by one common smart card.

5. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that
- the decoder device (STB) has an interface (PCI) via which the decoder device (STB) can be connected to a computer (PC), which is set up for controlling the decoder device (STB) and/or for establishing a connection to another subscriber via the telecommunications network (tel. network).

6. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that
- the control unit (RCU) is made up of the computer (PC), which
- has an interface (IR 3,6,7) for controlling the decoder device (STB); and
- an interface (IFD 3,6) for the identification and/or

key carrier component (ICC BC) for authorizing the connection via the telecommunications network (tel. network) and/or the identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB).

7. The decoder device (STB) having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the decoder device (STB) is integrated in the television set (TV).

8. A smart card for a decoder device having a control unit (RCU) as recited in one of the preceding claims, comprising

- a computer unit;
- a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card; and
- a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access,

characterized in that

- a general key is stored in the protected area of the second memory area, and under the control of the general key, the external host computer enters at least one further simple key, as well as a protocol program associated with this further simple key.

9. The smart card as recited in Claim 10, characterized

in that

- stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

10. A method for a host computer of a pay TV provider to communicate with a decoder device having a control unit (RCU) as recited in one of Claims 1 - 7, and a smart card according to Claim 8 or 9, characterized by the following steps:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;
- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card;
- the protected memory area of the smart card is inhibited.

11. The method as recited in Claim 10, characterized in that

- before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program are decrypted by the computer unit of the smart card.

12. The method as recited in Claim 10, characterized in that some of the data transmission traffic is transmitted

back and forth via the interface (5) to the telephone network, and some via a line (1), which is linked to the television set (TV) for transmitting the encrypted television program, together with or prior to a useful signal that reproduces the encrypted television program, the information to be transmitted being distributed and transmitted in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.